RECORDS AND BRIEFS

FILED
SEP 29 2017
OFFICE OF THE CLERK
SUPREME COURT, U.S.

No. 16-402

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,
PETITIONER,

v.

UNITED STATES OF AMERICA,
RESPONDENT.

On Writ of Certiorari to the
United States Court of Appeals for the Sixth Circuit

BRIEF OF *AMICUS CURIAE* MICHAEL VARCO IN SUPPORT OF RESPONDENT

Michael Varco
Counsel of Record and
Amicus Curiae
P.O. Box 2548
Reston, VA 20195
(703) 635-7903
m_varco@yahoo.com

September 29, 2017

QUESTION PRESENTED

Whether the government's acquisition, pursuant to a court order, of historical mobile-device location records maintained by a third party violates the Fourth Amendment rights of the individual owner of the mobile device to whom the records pertain.

TABLE OF CONTENTS

Page

QUESTION PRESENTED i

TABLE OF AUTHORITIES iii

INTEREST OF AMICUS CURIAE 1

BACKGROUND 3

SUMMARY OF ARGUMENT 4

ARGUMENT 7

I. The Digital Age Does Not Necessitate Changes to the Third-Party Doctrine. 7

A. Justice Sotomayor's Suggestion in *Jones* to Reconsider the Third-Party Doctrine Overlooks What the Government Learns from Other Sources and How Crime Harms Victims. 8

B. Cell Phone Users Have More Control Over Providing CSLI to Service Providers Than Crime Victims May Have Over Revealing Sensitive Information About Themselves. 13

C. The Third-Party Doctrine Is More Important Than Ever in the Digital Age Because of "Substitution Effects" 14

D. Laws Are the Best Way to Address Privacy Issues with the Third-Party Doctrine. 18

E. Markets Also Respond to Privacy Concerns from the Public. 19

II. The Past Use of Tracking Dogs to Determine Historical Location Information Is Analogous to Acquiring Historical CSLI. 20

III. People Lack a Reasonable Expectation of Privacy in Historical CSLI. 22

A. Before December 2010, Many Sources (e.g., FCC Rules, News, Manuals, Patents, and Movies) Informed the Public that Cell Phones Provided CSLI to Third Parties. 23

B. Today, People Have More Reasons to Know Their Cell Phones Provide CSLI to Third Parties. 25

Conclusion 26

TABLE OF AUTHORITIES

Page(s)

CASES

Citizens United v. Federal Election Com'n, 130 S.Ct. 876 (2010) 13

City of Los Angeles v. Patel, 135 S.Ct. 2443 (2015) 11

Communist Party of the United States v. SACB, 367 U.S. 1 (1961) 13

Page(s)

Florida v. Jardines,
133 S.Ct. 1409 (2013) 21, 22

Illinois v. Caballes,
125 S.Ct. 834 (2005) 21

Katz v. United States,
389 U.S. 347 (1967) 5

Kyllo v. United States,
533 U.S. 27 (2001). 22

New York ex rel. Bryant v. Zimmerman,
278 U.S. 63 (1928) 12

Smith v. Maryland,
442 U.S. 735 (1979) 7

United States v. Carpenter,
819 F.3d 880 (6th Cir. 2016) 3, 4, 5, 22

United States v. Diaz-Castaneda,
494 F.3d 1146 (9th Cir. 2007) 17

United States v. Jacobsen,
104 S.Ct. 1652 (1984) 21

United States v. Jones,
132 S.Ct. 945 (2012) 7, 8, 10, 11, 18, 22

United States v. Miller,
425 U.S. 435 (1976). 15

United States v. Place,
103 S.Ct. 2637 (1983) 21

United States v. Walraven,
892 F.2d 972 (10th Cir. 1989). 17

Page(s)

STATUTES

18 U.S.C. § 2703(d) 6, 11, 18, 19

CONSTITUTIONAL PROVISIONS

U.S. Const. amend. I..... 4, 11, 16, 17

U.S. Const. amend. IV .....passim

REGULATIONS

47 C.F.R. § 20.18..... 23, 24

OTHER AUTHORITIES

Accenture, *Banking Technology Vision 2017*, https://www.accenture.com/t20170322T205838Z__w__/us-en/_acnmedia/PDF-47/Accenture-Banking-Technology-Vision-2017.pdf#zoom=50. 16

ACLU, *Cell Phone Location Tracking Laws By State*, https://www.aclu.org/issues/privacy-technology/location-tracking/cell-phone-location-tracking-laws-state?redirect=map/cell-phone-location-tracking-laws-state..... 18

Apple, *Find My iPhone*, https://www.apple.com/icloud/find-my-iphone. 25

Apple, *iPhone User Guide* (2009), https://manuals.info.apple.com/MANUALS/0/MA616/en_US/iPhone_iOS3.1_User_Guide.pdf..... 7, 24

Page(s)

Ariel Barkhurst, *Robbers turn to rental cars to avoid detection*, AZ Sentinel, Apr. 12, 2012, http://articles.sun-sentinel.com/2012-04-03/news/fl-rental-cars-used-in-robberies-20120402_1_rental-cars-rental-vehicles-surveillance-cameras. 17

AT&T, *AT&T Transparency Report*, http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html. 8

Blake E. Reid, Comment, *Substitution Effects: A Problematic Justification for the Third-Party Doctrine of the Fourth Amendment*, 8 J. ON TELECOMM. & HIGH TECH. L. 613 (2010) 14

Ctr. for Medicare and Medicaid Serv., OMB No. 0938-0008, https://www.cms.gov/Medicare/CMS-Forms/CMS-Forms/downloads/cms1490s-english.pdf. 9

Devin Dwyer et al., *Rape Kit Testing Backlog Thwarts Justice for Victims*, ABC News, May 20, 2010, http://abcnews.go.com/Politics/sexual-assault-victims-congress-solve-rape-kit-backlog/story?id=10701295. 10

FBI, *Crime in the United States 2015*, https://ucr.fbi.gov/crime-in-the-u.s/2015/crime-in-the-u.s.-2015/tables/table-1 12

Page(s)

FCC, *FCC Report to Congress on the Deployment of E-911 Phase II Services By Tier III Service Providers* (Mar. 23, 2005), https://apps.fcc.gov/edocs_public/attachmatch/DOC-257626A1.pdf 23

James Barron, *How a Son of Sam Detective Realized 'This Has Got to Be the Guy'*, N.Y. Times, Aug. 6, 2017, https://www.nytimes.com/2017/08/06/nyregion/son-of-sam-killings-david-berkowitz.html. 16

Kim C. Thornton, Bloodhounds (1998) 5, 21

Libelium, *Meshlium Xtreme Technical Guide*, (v. 7.3, July 2017), http://www.libelium.com/downloads/documentation/meshlium_technical_guide.pdf 20

M. Licea, *Serial killer with shipping container dungeon: My victims had it coming*, N.Y. Post, Sept. 9, 2017, http://nypost.com/2017/09/09/serial-killer-says-he-was-trying-to-save-woman-he-kept-in-shipping-container 19

Mark Bergen, *Google Will Stop Reading Your Emails for Gmail Ads*, Bloomberg Tech., June 23, 2017, https://www.bloomberg.com/news/articles/2017-06-23/google-will-stop-reading-your-emails-for-gmail-ads. 19

NACVB, *Crime Victim Compensation: An Overview*, http://www.nacvcb.org/index.asp?bid=14. 9

Page(s)

Nat'l Archives, *From Benjamin Franklin to Richard Jackson, 25 June 1764*, https://founders.archives.gov/documents/Franklin/01-11-02-0064 21

Nate Anderson, *How "cell tower dumps" caught the High Country Bandits – and why it matters*, ARS Technica, Aug. 29, 2013, https://arstechnica.com/tech-policy/2013/08/how-cell-tower-dumps-caught-the-high-country-bandits-and-why-it-matters. 20

Orin Kerr, *Symposium: Carpenter and the Eyewitness Rule*, SCOTUSblog, (Aug. 4, 2017, 1:39 PM), http://www.scotusblog.com/2017/08/symposium-carpenter-eyewitness-rule. 11

Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009) 14

RAINN, *What is a Rape Kit?*, https://www.rainn.org/articles/rape-kit. 10

Ryan Hutchins, *Cell phone tracking software helps police, emergency workers*, NJ.com, Jun. 22, 2009, http://www.nj.com/news/index.ssf/2009/06/cell_phone_tracking_software_h.html. 25

Sup. Ct. D.C., *Crime Victims Compensation Program Brochure*, http://www.dccourts.gov/internet/documents/CVCP_Brochure.pdf. 9

Suspect in Kelsey Smith's Death Charged with Murder, Kidnapping, FoxNews.com, June 7, 2007, http://www.foxnews.com/story/2007/06/07/suspect-in-kelsey-smith-death-charged-with-murder-kidnapping.html 24

Tara C. Jatlaoui et al., *Abortion Surveillance - United States, 2013*, MMWR, Nov. 25, 2016, http://dx.doi.org/10.15585/mmwr.ss6512a1 9

The Recruit (Touchstone Pictures 2003) 25

U.S. Census Bureau, *Health Insurance Coverage in the US: 2015*, 1, https://www.census.gov/content/dam/Census/library/publications/2016/demo/p60-257.pdf 9

U.S. Patent No. 5,519,760 (filed June 22, 1994) 24

U.S. Patent No. 7,515,578 abs. (filed May 8, 2006) . 24

U.S. Patent No. 8,073,460 (filed Mar. 29, 2007) 24

Uber not the only ride-hailing company with sights set on driverless cars, AP, Sept. 18, 2016, https://www.cbsnews.com/news/uber-not-the-only-ride-hailing-company-with-sights-set-on-driverless-cars-lyft/. 17

Uber, *Ride*, https://www.uber.com/ride 25

Verizon, *United States Report*, http://www.verizon.com/about/portal/transparency-report/us-report. 8

Wash. Univ. in St. Louis, *Rape Trauma Syndrome*, https://rsvpcenter.wustl.edu/learn-more/rape-trauma-syndrome. 12

YouTube, *The Heist: Make Experience Your Business | Adobe Experience Cloud*, https://www.youtube.com/watch?v=_KOuliSqSJo..... 14

INTEREST OF AMICUS CURIAE[1]

As a crime victim, I have a personal obligation to share my concerns with this Court. While the constitutional rights of the accused matter, I do not want to see the interpretation of the Fourth Amendment change in a way that could hinder criminal investigations.

Also, I want this Court to understand how frustrating it has been to observe all the ways that companies track the locations of mobile devices – when users let them do so – only to see none of that information available to help me. Sharing my experience may help other crime victims too.

On July 31, 2016, I was a victim of an unprovoked assault in the Dupont Circle area of Washington DC. I suffered many fractures to my face and my jaw. The first two facial-trauma surgeons that I consulted could not perform the first surgery I needed. I cannot identify those involved with the assault; however, I hope that the detective assigned to my case may find more leads using cell-phone location information (CPLI). Herein, CPLI refers to location information based on one or more technologies (e.g., GPS, CSLI, Wi-Fi, etc.).

---

[1] Both parties have consented to all amicus briefs. No counsel for a party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than amicus curiae made a monetary contribution to its preparation or submission.

After the assault, I asked the detective to pursue relevant CPLI. I showed the detective a Google Timeline[2] from when the attack occurred. The Google Timeline showed a map of my phone's historical location, possibly from cellular and Wi-Fi signals my phone provided. The Google Timeline placed me at a 7-Eleven, steps from the assault. It indicated when I walked and when I took a vehicle. It placed me at the hospital later. When a nurse took a photo of me with my phone, Google put the photo on the Google Timeline. Because Google traced CPLI related to me, I thought Google – or another company – may have traced CPLI related to those near me during the crime. I thought relevant CPLI could identify people in the detective's video evidence.[3]

The detective requested the CPLI of those near me, but the prosecutor with decision-making authority declined the CPLI request. Fourth Amendment concerns may have been a factor in denying the CPLI request. For this reason, I hope that this Court will soon explain what limits, if any, an individual's Fourth Amendment rights put on the government acquiring CPLI from a third party to support a criminal investigation.

---

[2] For information about Google Timeline, see Google, *Google Maps Help*, https://support.google.com/maps/answer/6258979?co=GENIE.Platform%3DDesktop&hl=en.

[3] YouTube, *Persons of Interest in Aggravated Assault*. 1100 b/o 19th St. NW, on July 31, 2016, https://www.youtube.com/watch?v=MdrjECC1r1E&feature=youtu.be (uploaded May 16, 2017).

If this Court affirms the Sixth Circuit, then I hope that the government will use CPLI more effectively in criminal investigations, when appropriate. The government's capabilities for using CPLI in criminal investigations should catch up with other areas of forensics.

BACKGROUND

A jury convicted Timothy Ivory Carpenter and Timothy Michael Sanders of charges related to robberies in the Detroit area from December 2010 to April 2011. Based on cell phone numbers that one of their co-conspirators gave the FBI, the FBI applied for orders from magistrate judges to obtain cell-site location information (CSLI) from various wireless carriers without a warrant. The magistrate judges granted the FBI's requests for CSLI. The CSLI showed that Sander's and Carpenter's phones were within a half-mile to two miles of the location of each of the robberies around the time of the robberies.

The government used the CSLI at trial. Carpenter and Sanders appealed their convictions on the grounds that the government acquired the CSLI in violation of their Fourth Amendment rights. The Sixth Circuit affirmed both convictions, deciding that the government's acquisition of CSLI was not a search.[4]

---

[4] *United States v. Carpenter*, 819 F.3d 880, 884-86, and 890 (6th Cir. 2016).

SUMMARY OF ARGUMENT

Some would like this Court to believe that, due to new technologies in the digital age, an Orwellian state with constant surveillance is imminent.

This case does not justify those fears. In the present case, the government acquired historical cell-site location information (CSLI) to support a criminal investigation, not to track the public at large. In free societies, people expect their governments to investigate and prosecute criminal activity.

There are at least three reasons why this Court should decide the Fourth Amendment allows the government to acquire historical CSLI from a third party, pursuant to a court order.

First, the third-party doctrine should apply to CSLI. Under the third-party doctrine, a person lacks a reasonable expectation of privacy – and therefore lacks Fourth Amendment protection – in information voluntarily provided to a third party.[5] The third-party doctrine makes sense because a person's Fourth Amendment rights should not stop third parties from exercising their First Amendment rights and disclosing what they know to the government. Because cell phone users voluntarily provide CSLI to their service providers (i.e., third parties), cell phone users should not have Fourth Amendment protection in CSLI and/or other CPLI.

---

[5] *See id.* at 889.

Second, obtaining historic location information using dogs is analogous to CSLI; thus, dogs may be just as relevant as *Katz*.[6] CSLI could be considered a phone's digital scent trail, similar to a person's physical scent trail. Governments have used dogs for centuries to determine historic location information by tracking the physical scents of people. In fact, Benjamin Franklin tried to acquire bloodhounds in order to locate people accused of crimes.[7] Benjamin Franklin's past actions are relevant to colonial-era views about acquiring historical location information in criminal investigations. If the government does not need a warrant to determine a person's historical location by using a dog, then this Court should not require a warrant to determine the historical location of a device by acquiring CSLI.

Third, in addition to the reasons provided by the Sixth Circuit,[8] many other sources (e.g., news coverage, device manuals, movies, patents, FCC rules, etc.) show that people lack a reasonable expectation of privacy in historical CSLI.

---

[6] Part of the Sixth Circuit's opinion discusses *Katz* because CSLI does not belong to one of the protected elements in the text of the Fourth Amendment (e.g., persons, houses, papers, and effects). U.S. Const. amend. IV; *Carpenter*, 819 F.3d at 886 (deciding that the government's acquisition of CSLI was not a search, based on the two-part test in *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J. concurring)).

[7] Kim C. Thornton, *infra*, note 44 at 10.

[8] *Carpenter*, 819 F. 3d at 888 (discussing cell-signal strength indicators and roaming charges as CSLI indicators).

When deciding whether to apply the third-party doctrine to CSLI, this Court should consider the privacy and freedom interests of crime victims alongside those of crime suspects. Crime victims lose substantial privacy when they apply for crime victim's compensation, undergo rape kit exams, etc. Crime victims may have disfiguring injuries that reveal sensitive information to others. Results of crime, such as trauma and death, unjustly harm the associational and expressive freedoms of crime victims far more than CSLI could possibly harm crime suspects. Accordingly, in order to help law enforcement prosecute violent criminals and to prevent future crime victims, this Court should apply the third-party doctrine to CSLI.

Additionally, new technologies make the third-party doctrine more important than ever in the digital age. For example, artificial intelligence may replace human witnesses; consequently, law enforcement may have to rely on the third-party doctrine to obtain information that witnesses previously would have provided.

People that disagree with the current law can lobby Congress and/or state representatives to change the law. Alternatively, people can move to states that add a warrant requirement to 18 U.S.C. § 2703(d). This Court does not have to intervene.

Accordingly, the judgement of the Sixth Circuit Court of Appeals should be affirmed.

ARGUMENT

I. The Digital Age Does Not Necessitate Changes to the Third-Party Doctrine.

In modern times, third parties may use various technologies (e.g., CSLI, GPS, Wi-Fi) to determine the approximate locations of mobile devices (e.g., cell phones). The technologies determine the locations of mobile devices based on information the mobile devices provide to cell towers, GPS satellites, Wi-Fi access points, etc.[9]

Under the third-party doctrine, people have "no legitimate expectation of privacy" in information voluntarily given to third parties[10]; therefore, under prior precedents, a person's Fourth Amendment rights may not protect him from the government's acquisition of CPLI from third parties.

However, Justice Sotomayor has suggested revisiting the third-party doctrine in the digital age because of concerns that the government might use location monitoring to obtain extensive and intimate details about people.[11]

---

[9] *See* Apple, *iPhone User Guide*, p. 144 (2009), https://manuals.info.apple.com/MANUALS/0/MA616/en_US/iPhone_iOS3.1_User_Guide.pdf (describing Location Services).

[10] *Smith v. Maryland*, 442 U.S. 735 (1979).

[11] *United States v. Jones*, 132 S.Ct. 945, 955 (2012) (Sotomayor J., concurring) (citation omitted) ("Disclosed in [GPS] data . . . will be . . . trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel . . . .").

A. Justice Sotomayor's Suggestion in *Jones* to Reconsider the Third-Party Doctrine Overlooks What the Government Learns from Other Sources and How Crime Harms Victims.

The privacy issues that Justice Sotomayor discusses in *Jones* are minor compared to what the government learns from other sources and how crime impacts the privacy and freedoms of crime victims.

1. Medical Information

First, in *Jones*, Justice Sotomayor suggests that the government might infer people's medical information from location monitoring in criminal investigations.[12] Her concern overlooks how the government learns far more from its healthcare role and/or from crime victims than it could possibly infer from CSLI pertaining to crime suspects.

Many companies report how many location requests they receive. From July 2016 to June 2017, AT&T received 52,139 requests for historic CSLI.[13] In the first half of 2017, Verizon received 20,442 requests for location information, but a quarter had warrants.[14] It is unclear if any of the requests let the government infer medical information.

---

[12] *Id.*

[13] AT&T, *AT&T Transparency Report*, http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html.

[14] Verizon, *United States Report*, http://www.verizon.com/about/portal/transparency-report/us-report.

By comparison, the government learns far more from its healthcare role than it could possibly infer from historical CSLI. The US government covers health insurance for over 118 million people.[15] When the government pays a medical claim, the government learns someone's medical information (e.g., code for illness and test).[16] Also, since 1969 the CDC has kept detailed abortion statistics (e.g., mother's age, race, gestation, etc.).[17]

Also, crime victims reveal far more sensitive information to the government than the government could infer from CSLI. To apply for crime victim's compensation, crime victims may need to provide the government copies of their medical bills, lost wages, and mental-health bills.[18] The US pays "close to $500 million yearly to more than 200,000 victims" through crime victim compensation programs.[19]

---

[15] U.S. Census Bureau, *Health Insurance Coverage in the US: 2015*, tbl. 1, https://www.census.gov/content/dam/Census/library/publications/2016/demo/p60-257.pdf (2015 statistics).

[16] See e.g., Ctr. for Medicare and Medicaid Serv., *OMB No. 0938-0008*, https://www.cms.gov/Medicare/CMS-Forms/CMS-Forms/downloads/cms1490s-english.pdf.

[17] Tara C. Jatlaoui et al., *Abortion Surveillance - United States, 2013*, MMWR, Nov. 25, 2016, http://dx.doi.org/10.15585/mmwr.ss6512a1 (prepared by CDC).

[18] Sup. Ct. D.C., Crime Victims Compensation Program Brochure p. 3, http://www.dccourts.gov/internet/documents/CVCP_Brochure.pdf.

[19] NACVB, *Crime Victim Compensation: An Overview*, http://www.nacvcb.org/index.asp?bid=14.

Also, medical personnel perform about 180,000 sexual assault forensic exams yearly.[20] In those exams, crime victims may have to endure a full physical examination and/or may have to share their medical and sexual history – shortly after trauma.[21]

Because violent criminals may harm again, preserving the third-party doctrine may reduce how much private medical information the government learns about people; therefore, applying the third-party doctrine to CSLI is important. With the right tools, law enforcement may get the evidence it needs to convict more violent criminals; fewer violent criminals may harm fewer crime victims; and fewer crime victims may suffer impacts to their privacy.

2. Associational and Expressive Freedom

Second, in *Jones,* Justice Sotomayor expresses concern that the government might have unfettered discretion to track anyone; thus, "Awareness that the Government may be watching chills associational and expressive freedoms."[22] However, in the present case, the government's acquisition of historical CSLI pursuant to a court order poses little risk of moving this nation towards an Orwellian State.

---

[20] *See* Devin Dwyer et al., *Rape Kit Testing Backlog Thwarts Justice for Victims*, ABC News, May 20, 2010, http://abcnews.go.com/Politics/sexual-assault-victims-congress-solve-rape-kit-backlog/story?id=10701295.

[21] RAINN, *What is a Rape Kit?*, https://www.rainn.org/articles/rape-kit.

[22] *Jones,* 132 S.Ct. at 956 (citation omitted).

For starters, the government lacks unfettered discretion to track and/or acquire anyone's location information. Third parties may oppose government efforts to acquire the location information.[23] The law for CSLI requests, 18 U.S.C. § 2703(d), has limits: the information sought must be material to an ongoing criminal investigation; state laws may stop state governments from obtaining a court order; and service providers may challenge the court order.

Also, the historical CSLI at issue in the present case raises fewer concerns than the real-time tracking at issue in *Jones*. Historical CSLI cannot chill associational and expressive freedoms because the government acquires the CSLI after the crime suspect has already associated and expressed.

Conversely, allowing a crime suspect's Fourth Amendment rights to prevent a third party from sharing information with the government would chill expressive freedoms. Third parties have First Amendment rights to disclose information to the government.[24] If crime suspects could stop third parties from doing so, then crime suspects could chill the expressive freedoms of third parties.

---

[23] *See City of Los Angeles v. Patel*, 135 S.Ct. 2443 (2015). (holding a hotel that objects to giving the police a guest list must be able to have an impartial court review the request).

[24] Orin Kerr, *Symposium: Carpenter and the Eyewitness Rule*, SCOTUSBLOG, (Aug. 4, 2017, 1:39 PM), http://www.scotusblog.com/2017/08/symposium-carpenter-eyewitness-rule.

Plus, crime hurts associational and expressive freedoms far more than acquiring the historical CSLI of crime suspects possibly could. In 2015, around 1,197,704 violent crimes occurred in the US.[25] The murder victims lost their associational and expressive freedoms. The assault victims suffered injuries (e.g., a broken jaw or worse) that hurt their associational and expressive freedoms. Also, the rape victims suffered trauma-related symptoms such as social withdrawal, suspicion of strangers, etc.[26]

Because violent criminals may be repeat offenders, applying the third-party doctrine to CSLI promotes associational and expressive freedoms. With the right tools, law enforcement may convict more violent criminals; fewer violent criminals may harm fewer crime victims; and fewer crime victims may suffer harms to their associational and expressive freedoms.

Finally, even if the government's acquisition of CSLI causes some chilling effects, the government's interest may outweigh the alleged chilling effects. When the government's interest relates to reducing criminal activity, this Court has tolerated some burdens on expressive and associational freedoms.[27]

---

[25] FBI, *Crime in the United States 2015*, tbl. 1, https://ucr.fbi.gov/crime-in-the-u.s/2015/crime-in-the-u.s.-2015/tables/table-1.

[26] Wash. Univ. in St. Louis, *Rape Trauma Syndrome*, https://rsvpcenter.wustl.edu/learn-more/rape-trauma-syndrome.

[27] *New York ex rel. Bryant v. Zimmerman*, 278 U.S. 63, 75-77 (1928) (upheld law that made KKK disclose members because of KKK's violent history); *Communist Party of the United States v.*

Even in a non-criminal case, based on the government's interest to inform voters, this Court upheld a campaign-finance law that required a group to disclose its donors, despite concerns that the disclosure rules would expose donors to retaliation.[28]

B. Cell Phone Users Have More Control Over Providing CSLI to Service Providers Than Crime Victims May Have Over Revealing Sensitive Information About Themselves.

This Court may hear arguments that people do not voluntarily provide CSLI to service providers,[29] but that is incorrect. On a short-term or a long-term basis, people can avoid providing CSLI by leaving their phones at home, by turning their phones off, and/or by using non-cellular devices.

Many crime victims lack the same control. If crime victims have disfiguring and visible injuries, then others may see their injuries and may sense their pain. Those crime victims have hardly any control over revealing sensitive information about themselves. If preserving the third-party doctrine reduces the number of crime victims that end up in that situation, then it is worth keeping around.

SACB, 367 U.S. 1, 90-105 (1961) (Communist Party had to disclose its members so government could monitor subversion).

[28] *Citizens United v. Federal Election Com'n*, 130 S.Ct. 876, 916 and 980-82 (2010).

[29] One irony is this Court may hear the argument from an attorney whose phone is off and not providing CSLI.

C. The Third-Party Doctrine Is More Important Than Ever in the Digital Age Because of "Substitution Effects"

According to Orin Kerr's "Substitution Effects" theory, the third-party doctrine deters criminals from substituting public parts of their crimes (e.g., stalking a victim in person) with private transactions for criminal acts (e.g., calling victim on the phone).[30]

The following examples show how new technologies make the third-party doctrine more important than ever in the digital age. One key issue is that artificial intelligence may reduce the number of human witnesses available to provide information to law enforcement. Because robots and/or driverless cars may replace human witnesses, the third-party doctrine may become more important than ever in the digital age to investigate crimes.

1. Bank Robbery

Figure 1 is from a video of a fictitious bank robbery.[31] Although the robber wears a mask, the robber's phone reveals his identity to the bank. The teller recognizes the robber's picture on her monitor.

---

[30] Blake E. Reid, Comment, *Substitution Effects: A Problematic Justification for the Third-Party Doctrine of the Fourth Amendment*, 8 J. ON TELECOMM. & HIGH TECH. L. 613, 615 n. 8 (2010) (citing Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 573, 576 (2009)).

[31] YouTube, *The Heist: Make Experience Your Business | Adobe Experience Cloud*, https://www.youtube.com/watch?v=_KOuliSqSJo.

Figure 1 – Bank Robbery

Figure 1 shows how information that people give to a third party may aid criminal investigations. The robber's phone pinged the bank's system. If the robber evades capture, then the third-party doctrine may help the police determine the robber's identity.

Treating low-tech and high-tech sources of information differently, under the third-party doctrine, would lead to absurd results. As a low-tech example, under the third-party doctrine, the law-abiding customers at the bank have no Fourth Amendment protection in the bank's records of their deposits.[32] The government could acquire those deposit records without a warrant. If the third-party doctrine does not apply to the ping that the bank receives from the robber's phone (i.e., a high-tech source), then the government would need a warrant for the bank's records related to the robber's identity.

Granted, the bank teller could identify the robber for the police; however, the bank teller of the

---

[32] *United States v. Miller*, 425 U.S. 435 (1976).

future may be a robot instead of a person.[33] A robot teller may not have a First Amendment right to identify the robber. Because artificial intelligence may reduce the number of human witnesses that can give information to police, the third-party doctrine may become more important than ever in the digital age to discourage and investigate unlawful activity.

2. Son of Sam Killer Using Ride Service

Forty years ago, the Son of Sam killer terrified New York City. Location information from a parking ticket solved that case. The police checked parking ticket records for witnesses, but found a ticket for the killer's car instead. Police noticed the killer's ticket because of his out-of-town address.[34]

What would happen today if the killer went to and from the murders using a ride service instead of his own car? The killer would not receive a parking ticket: the police would have to find him another way. If the third-party doctrine remains valid, then police could acquire route and passenger logs from the ride service without a warrant. Also, the killer's driver could reveal the killer's information to police.

---

[33] About 76% of bankers think artificial intelligence will be the main way banks interact with customers in 3 years. Accenture, *Banking Technology Vision 2017*, pp. 22-23, https://www.accenture.com/t20170322T205838Z__w__/us-en/_acnmedia/PDF-47/Accenture-Banking-Technology-Vision-2017.pdf#zoom=50.

[34] James Barron, *How a Son of Sam Detective Realized 'This Has Got to Be the Guy'*, N.Y. TIMES, Aug. 6, 2017, https://www.nytimes.com/2017/08/06/nyregion/son-of-sam-killings-david-berkowitz.html.

However, ride services are developing autonomous cars to replace human drivers.[35] Autonomous cars may lack First Amendment rights to speak with the police; thus, the third-party doctrine may become more important than ever in the future to deter and investigate illegal activity.

If the third-party doctrine goes away, then ride services may be more desirable for criminals. A wanted criminal driving his own car may worry about capture when the police or a license-plate reader (LPR) check his license plate. Many lower courts do not consider license-plate checks a search.[36]

In contrast, using an autonomous car through a ride service may be less risky. Even if the police check the license plate of the autonomous car, police would need to rely on the ride service, or another source, for passenger details. If the third-party doctrine goes away, then a killer like the Son of Sam might use an autonomous car through a ride service to lower his risk of capture.[37]

---

[35] *Uber not the only ride-hailing company with sights set on driverless cars*, AP, Sept. 18, 2016, https://www.cbsnews.com/news/uber-not-the-only-ride-hailing-company-with-sights-set-on-driverless-cars-lyft/.

[36] *See e.g.*, *United States v. Diaz-Castaneda*, 494 F.3d 1146, 1150 (9th Cir. 2007); *United States v. Walraven*, 892 F.2d 972, 974 (10th Cir. 1989).

[37] *See* Ariel Barkhurst, *Robbers turn to rental cars to avoid detection*, AZ SENTINEL, Apr. 12, 2012, http://articles.sun-sentinel.com/2012-04-03/news/fl-rental-cars-used-in-robberies-20120402_1_rental-cars-rental-vehicles-surveillance-cameras.

D. Laws Are the Best Way to Address Privacy Issues with the Third-Party Doctrine.

Justice Alito's concurrence in *Jones* states: "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative" because a "legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[38]

Congress put several safeguards in 18 U.S.C. § 2703(d). Under 18 U.S.C. § 2703(d), the government must have "reasonable grounds" but not "probable cause" to acquire non-content records like CSLI without a warrant or the third party's consent. The third-party may file a motion to modify or quash a court order for CSLI. A judge reviews the request. Also, many state laws prevent state governments from acquiring CSLI without a warrant.[39]

The time period of CSLI requested should be a factor in deciding whether the request complies with 18 U.S.C. § 2703(d), not whether the CSLI request violates the Fourth Amendment. If the CSLI relates to a long-term crime spree, then a court could decide the government has "reasonable grounds" to request a long-term period of historical CSLI.

---

[38] *Jones*, 132 S.Ct. at 964 (Alito J., concurring in judgement).

[39] ACLU, *Cell Phone Location Tracking Laws By State*, https://www.aclu.org/issues/privacy-technology/location-tracking/cell-phone-location-tracking-laws-state?redirect=map/cell-phone-location-tracking-laws-state.

Accordingly, this Court does not have to exclude CSLI from the third-party doctrine. People that want to change 18 U.S.C. § 2703(d) can pressure Congress to change the law, try to change the law in their state, or they can move to a state that requires a warrant for CSLI.

E. Markets Also Respond to Privacy Concerns from the Public.

Markets also respond to the public's privacy preferences. For example, in order to attract more corporate customers, Google no longer scans the emails of free-gmail users to target ad content.[40]

If some people want more privacy protection, then they may reward companies that provide people more privacy protection. They may pressure companies to challenge government § 2703(d) orders more often. Other people, however, might appreciate the benefits from CSLI. CSLI helps service providers find weak spots in their networks and offer new services (e.g., navigation services). Also, CSLI helps solve crimes, locate 911 callers, and rescue people.[41]

---

[40] Mark Bergen, *Google Will Stop Reading Your Emails for Gmail Ads*, Bloomberg Tech., June 23, 2017, https://www.bloomberg.com/news/articles/2017-06-23/google-will-stop-reading-your-emails-for-gmail-ads.

[41] M. Licea, *Serial killer with shipping container dungeon: My victims had it coming*, N.Y. Post, Sept. 9, 2017, http://nypost.com/2017/09/09/serial-killer-says-he-was-trying-to-save-woman-he-kept-in-shipping-container (CSLI helped find victim).

Markets also develop technologies that may provide more-targeted options for acquiring CPLI. For example, since cell towers cover a large area, the government may acquire over 150,000 phone numbers from a cell tower dump.[42] On the other hand, because Wi-Fi Access Points have a limited range (e.g., ~200 meters) and just detect devices with the Wi-Fi radio on,[43] the government may receive the non-content information of far fewer people from a Wi-Fi Access Point. In some situations, instead of a cell tower, a Wi-Fi Access Point may be an alternative source for CPLI.

II. The Past Use of Tracking Dogs to Determine Historical Location Information Is Analogous to Acquiring Historical CSLI.

There are similarities between using tracking dogs and gathering CSLI to determine historical location information. CSLI could be considered a digital scent trail of a mobile device. The digital scent trail is analogous to a person's scent trail with one exception: people can avoid leaving a digital scent trail by leaving their device at home; however, people cannot avoid leaving a physical scent trail.

---

[42] Nate Anderson, *How "cell tower dumps" caught the High Country Bandits – and why it matters*, ARS Technica, Aug. 29, 2013, https://arstechnica.com/tech-policy/2013/08/how-cell-tower-dumps-caught-the-high-country-bandits-and-why-it-matters.

[43] Libelium, *Meshlium Xtreme Technical Guide*, pp. 170, 174, and 177 (v. 7.3, July 2017), http://www.libelium.com/downloads/documentation/meshlium_technical_guide.pdf.

Before Benjamin Franklin was a delegate at the Constitutional Convention of 1787, he requested bloodhounds to help settlors find people accused of crimes.[44] Benjamin Franklin's past actions are relevant to colonial-era views about the government gathering historical location information in criminal investigations. Also, dogs have been used since at least the 1300s to follow the scent trail of crime suspects.[45] Accordingly, this Court's cases on scent-tracking dogs are relevant to whether the Fourth Amendment protects CSLI.

In *Florida v. Jardines*, this Court held that the government's use of a drug-sniffing dog on the front porch and curtilage of a home to detect marijuana in the home was a "search" in violation of the Fourth Amendment."[46] Otherwise, the Fourth Amendment does not prevent the government from using dogs to investigate areas beyond the curtilage. Without a warrant, dogs may check luggage at an airport, check a substance that has fallen from a parcel in transit, and check a car during a lawful traffic stop.[47]

---

[44] Kim C. Thornton, Bloodhounds 10 (1998); *see also* Nat'l Archives, *From Benjamin Franklin to Richard Jackson*, 25 June 1764, https://founders.archives.gov/documents/Franklin/01-11-02-0064 (Benjamin Franklin wanted bloodhounds to track native Americans accused of plundering and kidnapping).

[45] *See Florida v. Jardines*, 133 S.Ct. 1409, 1424 (2013) (Alito J., dissenting) ("Scottish law from 1318 made it a crime to 'disturb a tracking dog . . . pursuing thieves or seizing malefactors.").

[46] *Id.* at 1409.

[47] *Id.* at 1417 (citing *United States v. Place*, 103 S.Ct. 2637 (1983), *United States v. Jacobsen*, 104 S.Ct. 1652 (1984), and

The process for acquiring the CSLI is different from the Fourth Amendment violation in *Jardines*. In *Jardines*, the police used a dog to detect marijuana in a person's home, trespassed onto the person's property, and acted without a court order.[48] When the government acquires CSLI pertaining to a person, the government acts pursuant to a court order and acquires business records from a third party without trespassing onto the person's property.

III. People Lack a Reasonable Expectation of Privacy in Historical CSLI.

Generally, "a Fourth Amendment search occurs when the Government violates a subjective expectation of privacy that society recognizes as reasonable."[49] Also, trespasses upon a person, the person's house, the person's papers, and the person's effects count as a search.[50]

The Sixth Circuit's opinion provides several reasons why the government's acquisition of historical CSLI from a third party is not a search.[51]

Illinois v. Caballes, 125 S.Ct. 834 (2005)).

[48] *Id.* at 1413.

[49] *Kyllo v. United States*, 533 U.S. 27, 33 (2001).

[50] *Jones*, 132 S.Ct. at 950.

[51] *Carpenter*, 819 F.3d at 887-90 (holding the government's acquisition of CSLI was not a search because cell phone users (i) lack a property interest in historical CSLI, (ii) have lower privacy expectations in business records and routing (non-content) information, and (iii) should know their phone provides its location because of signal indicators and roaming charges).

However, there are more facts that bolster the Sixth Circuit's discussion on why people lack a reasonable expectation of privacy in historical CSLI. Because the present case concerns historical CSLI from December 2010 to April 2011, this brief discusses the facts known before December 2010 separately from the facts known today.

A. Before December 2010, Many Sources (e.g., FCC Rules, News, Manuals, Patents, and Movies) Informed the Public that Cell Phones Provided CSLI to Third Parties.

Before December 2010, most people knew or should have known that their cell phones provided CSLI to service providers.

First, based on Federal Communication Commission (FCC) rules, cell phone users around December 2010 should have expected no location privacy when they made 911 calls. By extension, cell phone users should have expected that the government could acquire CSLI for other purposes. In 1996, the FCC crafted rules to ensure wireless carriers would provide the location of wireless 911 callers to 911 call centers.[52] By October 1, 2001, the FCC started Phase II Emergency 911 (E-911) service requirements on wireless carriers.[53]

---

[52] See FCC, *FCC Report to Congress on the Deployment of E-911 Phase II Services By Tier III Service Providers*, p. 1 n. 3 (Mar. 23, 2005), https://apps.fcc.gov/edocs_public/attachmatch/DOC-257626A1.pdf.

[53] 47 C.F.R. § 20.18(e) to (h).

Effective December 31, 2005, the FCC's Phase II E-911 regulations require all new cell phones must be location-capable (i.e., have location-determining hardware and/or software for the wireless carrier to determine the cell phone's location for a 911 call).[54] The FCC's Phase II E-911 rules also set location-accuracy requirements that the wireless carriers must meet by certain target dates.[55]

Second, multiple sources explained that cell phones provided location information to others. Service contracts are one example.[56] Patents[57] and device manuals are other sources. An iPhone® user guide from 2009 discloses several phone features: the phone gives directions based on the phones current location; the phone provides location information during 911 calls; the phone tags photos with location information; and the phone lets users manage their location services.[58]

Even if the average person did not read FCC regulations, product manuals, or patents, news reports informed the public that cell phones provided location information to service providers.[59]

---

[54] 47 C.F.R. § 20.18(g)(1)(v).

[55] 47 C.F.R. § 20.18(h) (target dates are after January 18, 2011).

[56] U.S. Patent No. 8,073,460 col. 7 l. 7-30 (filed Mar. 29, 2007).

[57] *See e.g.*, U.S. Patent No. 5,519,760 abs. (filed June 22, 1994) and U.S. Patent No. 7,515,578 abs. (filed May 8, 2006).

[58] Apple, *supra*, note 9, at pp. 24, 51, 103, 114-19, and 144.

[59] *See e.g., Suspect in Kelsey Smith's Death Charged with Murder, Kidnapping*, FoxNews.com, June 7, 2007, http://www

Movies also notified the public. The Recruit, a 2003 spy thriller that grossed over $52 million in US sales, included a scene where CIA agents tracked the main character's location based on his cell phone.[60] Thus, by 2010, people knew or should have known that cell phones provided CSLI to third parties.

B. Today, People Have More Reasons to Know Their Cell Phones Provide CSLI to Third Parties.

People today have more reasons to know that their cell phones provide CSLI to third parties. With ride-sharing services, people can arrange for vehicles to pick them up at locations their phones provide. While people wait, their phones show the location of the driver's vehicle.[61] Applications help people find their lost or stolen phone.[62] Accordingly, it is hard to imagine how any cell phone users would be unaware that their cell phones provide CSLI to third parties.

.foxnews.com/story/2007/06/07/suspect-in-kelsey-smith-death-charged-with-murder-kidnapping.html ("[L]aw enforcement put search teams within a four-mile radius of where the body was found, based on the cell phone signals."); Ryan Hutchins, *Cell phone tracking software helps police, emergency workers*, NJ.com, Jun. 22, 2009, http://www.nj.com/news/index.ssf/2009/06/cell_phone_tracking_software_h.html.

[60] The Recruit (Touchstone Pictures 2003) (At the end, Dennis tells James, "You forgot to turn your cell phone off. That's how we tracked you: your cell phone.").

[61] *See e.g.*, Uber, *Ride*, https://www.uber.com/ride.

[62] *See e.g.*, Apple, *Find My iPhone*, https://www.apple.com/icloud/find-my-iphone.

Conclusion

For the foregoing reasons, the judgment of the Sixth Circuit Court of Appeals should be affirmed.

Respectfully submitted.

Michael Varco
Counsel of Record and
Amicus Curiae
P.O. Box 2548
Reston, VA 20195
(703) 635-9703
m_varco@yahoo.com

September 29, 2017